МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3, 4
Семестр	6, 7

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
25.01.2022, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.01.2022 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
начальник отдела информационной
безопасности «КУБ» (АО) , _____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Техническая защита информации» является формирование профессиональных навыков обеспечения информационной защиты от съема информации по техническим каналам утечки информации, использования методов и средств инженерно-технической защиты информации и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Техническая защита информации» рассматривает основные принципы и основные направления технической защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Защита информации от утечки по техническим каналам входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Физика

Основы радиотехники

Теория информации

Основы информационной безопасности

Электроника и схемотехника

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Управление информационной безопасностью

Аттестация АИС

Тестирование систем защиты информации автоматизированных систем

Подготовка к сдаче и сдача государственного экзамена

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы проектирования систем защиты распределенных информационных систем

Производственная - практика по получению профессиональных умений и опыта профессиональной деятельности

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Производственная - научно-исследовательская работа

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Форензика

Моделирование систем защиты информации

Производственная - преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Защита информации от утечки по техническим каналам» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с	

нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	
ОПК-6.1	Организует защиту информации ограниченного доступа в автоматизированных системах
ОПК-6.2	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем
ОПК-6.3	Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	
ОПК-9.1	Использует технические средства защиты информации
ОПК-9.2	Применяет современные средства защиты сетей и систем защиты информации

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 7 зачетных единиц 252 акад. часов, в том числе:

– контактная работа – 142,45 акад. часов:

– аудиторная – 136 акад. часов;

– внеаудиторная – 6,45 акад. часов;

– самостоятельная работа – 73,85 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - зачет, курсовой проект, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие положения защиты информации техническими средствами								
1.1 Предмет и содержание дисциплины. Физические основы функционирования систем обработки и передачи информации	6	2	3		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к тестированию	Контрольное тестирование	
1.2 Задачи защиты информации от утечки по техническим каналам.		1	2		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к тестированию	Контрольное тестирование	
1.3 Методы и средства инженерной защиты объектов. Системы охранно-тревожной сигнализации. Системы пожарной сигнализации		1	1		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	

Итого по разделу		4	6		7			
2. Технические каналы утечки информации								
2.1 Условия и особенности утечки информации.Структура канала утечки. Виды технических каналов утечки информации	6	3	4		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	
2.2 Условия образования каналов утечки. Характеристики каналов утечки информации		2	4/2И		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	
Итого по разделу		5	8/2И		10			
3. Акустический канал утечки информации								
3.1 Виды акустических каналов утечки информации. Способы перехвата и средства съема информации по акустическому каналу	6	2	5/3И		10	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	
3.2 Способы и средства защиты от съема информации по акустическому каналу.Системы защиты от утечки информации по акустическому каналу		2	5/0,9И		10	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	
Итого по разделу		4	10/3,9И		20			
4. Вибрационный канал утечки информации								

4.1 Виды вибрационных каналов утечки информации. Способы перехвата и средства съема информации по вибрационному каналу	6	2	5/3И		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
4.2 Способы и средства защиты от съема информации по вибрационному каналу.Системы защиты от утечки информации по вибрационному каналу.		2	5/3И		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
Итого по разделу		4	10/6И		7			
5. Зачет								
5.1 Подготовка к зачету	6				12,05	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету	Зачет	
Итого по разделу					12,05			
Итого за семестр		17	34/11,9И		56,05		зачёт	
6. Оптический канал утечки информации								
6.1 Виды оптических каналов утечки информации. Способы перехвата и средства съема информации по оптическому каналу	7	4	4/2И		2	ное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	

6.2 Способы и средства защиты от съема информации по оптическому каналу. Системы защиты от утечки информации по оптическому каналу		4	4/2И		1	ное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
Итого по разделу		8	8/4И		3			
7. Электросетевой канал утечки информации								
7.1 Виды электросетевых каналов утечки информации. Способы перехвата и средства съема информации по электросетевому каналу	7	4	4/2И		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
7.2 Способы и средства защиты от съема информации по электросетевому каналу. Системы защиты от утечки информации по электросетевому каналу		4	4/3И		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
Итого по разделу		8	8/5И		7			
8. Электромагнитный канал утечки информации								
8.1 Виды электромагнитных каналов утечки информации. Способы перехвата и средства съема информации по электромагнитному каналу.	7	6	6/5,85И		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	

8.2 Способы и средства защиты от съема информации по электромагнитному каналу. Системы защиты от утечки информации по электромагнитному каналу		4	8/2И		0,5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
Итого по разделу		10	14/7,85И		2,5			
9. Поиск средств несанкционированного съема информации								
9.1 Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях.	7	4	11/1И		1	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
9.2 Контроль эффективности мер по защите информации техническими средствами		4	10		4,3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	
Итого по разделу		8	21/1И		5,3			
10. Экзамен								
10.1 Экзамен	7					Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену.	Экзамен	
Итого по разделу								

Итого за семестр	34	51/17,85И		17,8		экзамен,кп	
Итого по дисциплине	51	85/29,75И		73,85		зачет, курсовой проект, экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

c) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

d) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Разделно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ

ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся с использованием *методов IT*.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а также с применением *Кейс-технологий*.

Задания и вопросы по разделам

Раздел 1-4

Вопросы:

1. Виды, источники и носители защищаемой информации.
2. Опасные сигналы и их источники.
3. Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
4. Характеристики технических каналов утечки информации.
5. Комплексное использование каналов утечки информации.
6. Средства обнаружения и локализации закладных устройств.
7. Материально-вещественные каналы утечки информации.
8. Задачи защиты информации от утечки по техническим каналам.
9. Одноканальный канал утечки информации.
10. Носители информации в акустическом канале.

Задания:

1. Маскирование речевых сигналов акустическими шумами с использованием системывиброакустической и акустической защиты Соната-АВ (модель 3М).
2. Защита речевой информации от съема по вибрационному каналу с использованием системывиброакустической и акустической защиты Соната-АВ (модель 3М).
3. Вычислить мощность радиосигнала в канале CDMAс использованием анализатора спектра «АКС-1301».

Раздел 5-8

Вопросы:

1. Случайные опасные сигналы.
2. Диапазоны частот радиоэлектронного канала.
3. Носители информации в оптическом канале.
4. Оптические диапазоны частот.
5. Электрические приборы, создающие случайные опасные сигналы.
6. Пропускная способность канала.
7. Перехват акустических колебаний:через ВТСС, обладающих “микрофонным эффектом”.
8. Стетоскопы, комплексированные с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн.
9. Перехват акустических сигналов путем:лазерного зондирования оконных стекол.

Задания:

1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Касандра».
2. Обнаружение устройств и анализ сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Касандра».
3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в помещении с использованием генератора радиошума ГШ-1000М.
4. Обеспечить подавление нормальной работы телефонных закладок любых типов подключения во время переговоров с использованием устройства защиты Прокруст 2000.
5. Обеспечить защиту линий электропитания и заземления от утечки информации с использованием устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2».

7 Оценочные средства для проведения промежуточной аттестации

Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Компетенция / Индикатор достижения компетенции	Оценочные средства
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	
ОПК-6.1 Организует защиту информации ограниченного доступа в автоматизированных системах	Вопросы к экзамену 1. Характеристики способов и средств наблюдения в оптическом диапазоне. 2. Характеристики зрительной системы человека. 3. Виды и характеристики объективов. 4. Визуально-оптические приборы (бинокли, трубы. Телескопы) 5. Приборы ночного видения и тепловизоры. 6. Способы и средства наблюдения в радиодиапазоне. 7. Задачи, решаемые при перехвате сигналов и структура типового комплекса для перехвата. 8. Виды и характеристики антенн. 9. Радиоприёмники и их характеристики. 10. Способы и средства прослушивания, слуховая система человека. 11. Стетоскопы и телефонные закладки. 12. Метод ВЧ-навязывания и его применение для добывания информации. 13. Характеристики закладных устройств, затрудняющие их обнаружение. 14. Средства и методы (не меньше двух) обнаружения закладных устройств. **Вопросы для зачета** 1. Направленные и лазерные микрофоны. 2. Типы микрофонов и их характеристики. 3. Закладные устройства и их характеристики. 4. Требования защиты информации. 5. Методы и средства защиты речевой информации. 6. Физические АЭП - преобразователи – источники опасных сигналов. 7. Характеристики технических каналов утечки информации. 8. Пассивные и активные методы защиты информации в акустическом канале. 9. Материально-вещественные каналы утечки информации

ОПК-6.2 Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Вопросы к экзамену 1. Способы подключения и защита телефонной линии. 2. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него. 3. Беззаходовые методы прослушивания помещений по ТЛ. 4. Мобильные системы связи и их использование в информационных атаках. 5. Защита информации от атак с помощью сотовых телефонов и диктофонов. 6. Оптические каналы утечки информации (атака и защита). 7. Радиоэлектронные каналы утечки информации. 8. Пассивные и активные методы защиты информации в радиоэлектронном канале. 9. Способы и принципы инженерно технической защиты информации. 10. Способы и средства инженерной защиты и технической охраны объектов. 11. Утечка информации по ПЭМИН и применяемые меры защиты. 12. Зоны электромагнитного поля и возможности утечки информации. 13. Контролируемая зона и критерий защищённости СВТ.
ОПК-6.3 Применяет нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	1. С использованием графического метода рассчитать радиус зоны R2 для ЭВТ. 2. Рассчитать показатель защищенности технических средств обработки и передачи цифровой речи по каналу ПЭМИ. 3. Рассчитать показатель защищенности цифровой речи в радиоканале. 4. Для представленной схемы помещения выбрать контрольные точки (КТ) и разработать схемы измерений по акустическому каналу для этих КТ. 5. Проанализировать математическую модель утечки речевой информации по акустическому каналу. 6. Проанализировать математическую модель утечки речевой информации по виброакустическому каналу. 7. Проанализировать математическую модель утечки речевой информации по каналам, использующим перехват электромагнитных и электрических сигналов. 8. Проанализировать математическую модель утечки речевой информации по лазерному каналу
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	

ОПК-9.1 Использует технические средства защиты информации	Задания: 1. Замаскировать речевые сигналов акустическими шумами в аудитории с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 2. Обеспечить защиту речевой информации от съема по вибрационному каналу в аудитории с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 3. Вычислить мощность радиосигнала в канале CDMA с использованием анализатора спектра «АКС-1301». 4. Настроить СЗИ Соната-АВ. 5. Провести исследование систем активного зашумления и расчет показателей их эффективности с использованием комплекса «Сигурд». 6. Рассчитать отношения «сигнал/шум» в отходящих линиях с использованием комплекса «Сигурд». 7. С использованием комплекса «Кассандра» определить количество пиковых сигналов в заданном диапазоне частот. Провести полный анализ каждого пикового сигнала. Установить пояснительные метки на все пиковые сигналы. Вывести спектрограмму заданного диапазона частот, графики накопленных максимумов. Найти сигнал максимальной мощности и пометить его. 8. С использованием комплекса «Кассандра» в заданном диапазоне частот регистрировать и заносить в список слабые шумоподобные сигналы. Регистрировать факт наличия излучения на заданной частоте. Провести анализ определения линии порога с использованием критерия «идеального наблюдателя» и критерия Неймана-Пирсона. Обосновать способ создания линии порога. 9. Найти радиозакладку с помощью комплекса радиомониторинга «Кассандра». 10. С использованием комплекса «Кассандра» создать базу данных легальных сигналов и создать на ее основе эталонную панораму частот. Найти разность эталонной и текущей панорам.
ОПК-9.2 Применяет современные средства защиты сетей и систем защиты информации	Задания: 1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Кассандра». 2. Обнаружить устройства и проанализировать сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Кассандра».

	3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в аудитории МГТУ с использованием генератора радиошума ГШ-1000М. 4. Обеспечить подавление нормальной работы телефонных закладок любых типов подключения во время переговоров с использованием устройства защиты Прокруст 2000 в аудитории МГТУ. 5. Провести исследование ТС на наличие информативных сигналов ПЭМИН с использованием комплекса «Сигурд». 6. Произвести расчет показателей защищенности технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами сиспользованием комплекса «Сигурд». 7. Проверить работоспособность генератора шума ГШ-1000М для защиты информации от утечки за счёт побочныхэлектромагнитных излучений. 8. Проверить работоспособность устройства защитыПрокруст 2000. 9. Проверить работоспособность устройства дляподавления сигнала сотовой связи.

Темы курсовых работ:

1. Расчет выполнения норм противодействия акустической речевой разведке для выбранного помещения МГТУ.
2. Проектирование эффективного комплекса защиты акустической информации для выбранного помещения МГТУ.
4. Расчет выполнения норм виброакустической защищенности для выбранного помещения МГТУ.
5. Оценка защищенности средств вычислительной техники от утечки информации засчет ПЭМИ для выбранного помещения МГТУ.
7. Аналитическое обоснование необходимости разработки системы технической защиты информации на основе специального исследования выделенного помещения набазе МГТУ.
8. Экспериментальное исследование и расчет основных параметров воздушного канала утечки информации.
9. Экспериментальное исследование и расчет основных параметровакустоэлектрического канала утечки речевой информации.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Показатели и критерии оценивания зачета:

– на «зачтено» – обучающийся должен показать пороговый уровень знаний на уровневоспроизведения и объяснения информации**;**

– на «не зачтено» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации**.**

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные

навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

Показатели и критерии оценивания курсовой работы:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения ин-формации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Баранкова И.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс]: учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов; МГТУ. - Магнитогорск: МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true . - Макрообъект*.

2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 24.01.2022)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты

б) Дополнительная литература:

1. Румянцев, К. Е. Алгоритмы обнаружения источников оптического излучения : учебник / К. Е. Румянцев ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 232 с. - ISBN 978-5-9275-3201-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1088145 (дата обращения: 26.02.2022)

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 24.01.2022).

в) Методические указания:

1. Баранкова И.И. Применение комплекса радиомониторинга для постобработки спектограмм [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 18 с.

2. Баранкова И.И. Защита телефонных линий с использованием прибора «Прокруст-2000» [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности

10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Калугина О.Б., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 20 с.

3. Баранкова И.И. Поиск радиозакладок с применением комплекса радиомониторинга [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 12 с.

4. Баранкова И.И. Использование комплекса радиомониторинга для построения графиков текущих значений сканируемых частот [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 18 с.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-162-21 от 26.03.2021	26.03.2023
NotePad++	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Архив научных журналов «Национальный электронно-информационный концорциум» (НП НЭИКОН)	https://archive.neicon.ru/xmlui/
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Международная база полнотекстовых журналов	http://link.springer.com/
Международная реферативная и полнотекстовая справочная	http://scopus.com
Университетская информационная система	https://uisrussia.msu.ru
Федеральный образовательный портал –	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И.	https://magtu.informsystema.ru/Marc.html?locale=ru
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лаборатория технической защиты информации (ауд. 2122):

1. АКС-1301 Анализатор спектра
2. Комплекс радиомониторинга "Касандра К6" с диапазоном рабочих частот 0,009-6000Мгц
3. Комплекс радиомониторинга "Касандра К21" с диапазоном рабочих частот 0,009-21000Мгц
4. Генератор шума стационарный "ГШ-1000-М"
5. Система виброакустической и акустической защиты "Соната-АВ"
6. Устройство защиты телефонных переговоров от прослушивания и записи "Прокруст-200"
7. Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»
8. Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Лекционные аудитории (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.):

Мультимедийные средства хранения, передачи и представления информации

Компьютерные классы (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.):

Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы проводятся в компьютерных классах или специализированных лабораториях с целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий лабораторной работы используйте лекции, справочный материал программного обеспечения, рекомендованную литературу и цифровые образовательные ресурсы соответствующих методических материалов, размещенных в сети Интернет или локальной сети университета. Перед выполнением лабораторной работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению лабораторной работы, внимательно прочтите рекомендации к ее выполнению. Ознакомьтесь с перечнем рекомендуемой литературы, повторите теоретический материал, относящийся к теме работы. Ответьте на контрольные вопросы, выполните задания для самостоятельного выполнения. По результатам лабораторной работы предоставляется отчет. Отчет к лабораторным работам должен содержать:

- название лабораторной работы;
- цель и задачи работы;
- краткие теоретические сведения;
- задания по лабораторной работе;
- ход работы - описание последовательности действий при выполнении работы;
- выводы или результаты.

Результаты выполнения лабораторной работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий лабораторной работы можно сохранить на образовательном портале в личном кабинете и использовать при подготовке к экзамену.

Защита работы и результаты оценивания.

Защита проводится в два этапа:

1. Демонстрируются результаты выполнения задания. В случае выполнения лабораторной работы, предусматривающей разработку программы, при помощи тестового примера доказывается, что результат, получаемый при выполнении программы, является правильным.
2. Для защиты работы студенту необходимо ответить на дополнительные вопросы преподавателя. Каждая лабораторная работа оценивается определенным количеством баллов исходя из 5-бальной системы оценок.

Лабораторная работа считается выполненной и защищенной, если выполнены все задания и даны правильные ответы преподавателю на заданные вопросы. Лабораторная работа считается выполненной и незащищенной, если выполнены все задания, но полученные результаты являются неверными или не даны правильные ответы преподавателю на заданные вопросы и ответы были не полные. Обучающемуся, не выполнившим в полном объеме все задания лабораторной работы, или пропустившим по уважительной причине лабораторную работу, необходимо выполнить ее самостоятельно в компьютерном классе или специализированной лаборатории, результаты выполненной работы сохранить на съемном накопителе или на образовательном портале. Результаты предоставить в сроки, указанные преподавателем вместе с отчетом, демонстрацией полученных результатов в компьютерном классе (или специализированной лаборатории) или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся при проведении лабораторных работ:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности и противопожарным мерам.

2. Обучающийся должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах или специализированных лабораториях университета.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки,хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем),электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленнымитребованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляетпосле замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочныесредства для проведения промежуточной аттестации» данной РПД.